



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>G06K</b>		<b>A2</b>	(11) International Publication Number: <b>WO 95/14283</b>				
			(43) International Publication Date: 26 May 1995 (26.05.95)				
(21) International Application Number: PCT/US94/12426		(81) Designated States: AU, CA, JP, KR, NO, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).					
(22) International Filing Date: 28 October 1994 (28.10.94)		<b>Published</b> <i>Without international search report and to be republished upon receipt of that report.</i>					
(30) Priority Data: 148,716 8 November 1993 (08.11.93) US							
(71) Applicant: HUGHES AIRCRAFT COMPANY [US/US]; 7200 Hughes Terrace, Los Angeles, CA 90045 (US).							
(72) Inventors: BATHRICK, Erwin, W.; 315 East Blossom Place, Brea, CA 92621 (US). GARBER, John, W.; 691 Santa Maria Lane, Davidsonville, MD 21035 (US). HUANG, Cheng-Chi; 7 Mountain Ash, Irvine, CA 92714 (US). KUNG, Kenneth, C.; 19029 Vickie Avenue, Cerritos, CA 90701 (US). MATTHEWS, Todd, E.; 2508 Jacaranda Street, Santa Ana, CA 92701 (US). ZUMDA, James, E.; 22136 Elsberry Way, Lake Forest, CA 92630 (US). MATTHEWS, Regina, L.; 5250 Avenida Despacio, Yorba Linda, CA 92687 (US).							
(74) Agents: WALDER, Jeannette, M. et al.; Hughes Aircraft Company, P.O. Box 80028, Building C1, M/S A126, Los Angeles, CA 90080-0028 (US).							
(54) Title: PROTECTED DISTRIBUTION PROTOCOL FOR KEYING AND CERTIFICATE MATERIAL							
(57) Abstract							
<p>Disclosed is a computer system and a method for the protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain, comprising the steps of sending keying material, including a password, generated by the Certifying Authority to the entity via a secure medium; generating and protecting, by the entity, a public and a private key pair using the keying material provided it by the certifying authority; generating, protecting and sending a request for a certificate to the certifying authority using the keying material provided it by the certifying authority; requesting, by the certifying authority, that the public key and address of the entity be sent to the certifying authority; protecting and sending the public key and address of the entity to the certifying authority using the keying material provided it by the certifying authority; assembling and issuing the certificate to the entity from the certifying authority and recording the public key of the entity at the certifying authority for public use within the domain of the certifying authority.</p>							
<table border="0"> <thead> <tr> <th style="text-align: center;"><u>CERTIFICATE</u></th> <th style="text-align: center;"><u>ENTITY</u></th> </tr> </thead> <tbody> <tr> <td style="vertical-align: top;"> <p>PREPARE INITIAL KEY MATERIAL FOR ENTITY</p> <p>OPERATION: ADD HOST (GENERATE KEY) WRITE SNMPcpg FILES (WITH KEY) SNMP REQUESTS HOST PUBLIC KEY</p> <p>GENERATE CERTIFICATE SIGN CERTIFICATE SNMP SET CERTIFICATE CA PUBLIC KEY</p> </td> <td style="vertical-align: top;"> <p>USER ENTERS PASSWORD (KEY MATERIAL) WRITE SNMPcpg FILES (WITH KEYS) GENERATE PUBLIC/PRIVATE KEY PAIR SEND STARTUP TRAP</p> <p>PREPARE AND SEND PUBLIC KEY</p> <p>SAVE CERTIFICATE CA PUBLIC KEY</p> </td> </tr> </tbody> </table>				<u>CERTIFICATE</u>	<u>ENTITY</u>	<p>PREPARE INITIAL KEY MATERIAL FOR ENTITY</p> <p>OPERATION: ADD HOST (GENERATE KEY) WRITE SNMPcpg FILES (WITH KEY) SNMP REQUESTS HOST PUBLIC KEY</p> <p>GENERATE CERTIFICATE SIGN CERTIFICATE SNMP SET CERTIFICATE CA PUBLIC KEY</p>	<p>USER ENTERS PASSWORD (KEY MATERIAL) WRITE SNMPcpg FILES (WITH KEYS) GENERATE PUBLIC/PRIVATE KEY PAIR SEND STARTUP TRAP</p> <p>PREPARE AND SEND PUBLIC KEY</p> <p>SAVE CERTIFICATE CA PUBLIC KEY</p>
<u>CERTIFICATE</u>	<u>ENTITY</u>						
<p>PREPARE INITIAL KEY MATERIAL FOR ENTITY</p> <p>OPERATION: ADD HOST (GENERATE KEY) WRITE SNMPcpg FILES (WITH KEY) SNMP REQUESTS HOST PUBLIC KEY</p> <p>GENERATE CERTIFICATE SIGN CERTIFICATE SNMP SET CERTIFICATE CA PUBLIC KEY</p>	<p>USER ENTERS PASSWORD (KEY MATERIAL) WRITE SNMPcpg FILES (WITH KEYS) GENERATE PUBLIC/PRIVATE KEY PAIR SEND STARTUP TRAP</p> <p>PREPARE AND SEND PUBLIC KEY</p> <p>SAVE CERTIFICATE CA PUBLIC KEY</p>						

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

**PROTECTED DISTRIBUTION PROTOCOL  
FOR KEYING AND CERTIFICATE MATERIAL**

**BACKGROUND OF THE INVENTION**

**1. Field of the Invention**

This invention relates in general to computer security systems, and, more particularly, to a computer security system and a method for the protected distribution of certificate and keying material between a certification authority and an entity in the certification authority's domain.

**2. Description of the Related Art**

In existing methods for distribution of certificate and keying material, the administrator must manually distribute the information to each end system (entity) and user. Administrators in the past were required to visit each system or user on the system more than once to initialize the information required to support the network security mechanism.

The certificate or keying material is used later to authenticate and to protect the communications between distributed entities. If these materials are compromised in the initial distribution, then the confidentiality and authentication services cannot be assured during further operation.

This manual distribution system is further fraught with difficulties in maintaining security in the physical transportation of the keying materials between the Certification Authority and the various entities, and with the consequent time lag mandated by the actual wait times involved in moving from one entity to the other. All during this setup time, the various entities are denied access to the protected data for which they may have an immediate need.

The present invention meets and overcomes this problem of maintaining security during the transfer of the keying

1 materials between entities and shortens the time during  
2 which access is denied an otherwise authorized entity to a  
3 minimum.

4 The present invention reduces the required visits  
5 needed to install the necessary security access software to  
6 a single visit by using a password (shared secret) to  
7 generate the essential keying material to be used for both  
8 integrity and encryption services to protect the data  
9 necessary for authentication and network security protocol  
10 protection.

#### 11 OBJECTS AND SUMMARY OF THE INVENTION

12 Therefore, it is an object of the present invention to  
13 provide a computer security network system and a method for  
14 the protected distribution of certificate and keying  
15 material between a certification authority and an entity in  
16 the certification authority's domain.

17 It is still another object of the present invention to  
18 provide a method and system that quickly provides  
19 authorized users control of their data.

20 It is another object of the present invention to  
21 provide a method and system that facilitates, rather than  
22 prevents, the establishment of encoded public and private  
23 key data or documents classified at different security  
24 levels.

25 The present invention provides a computer system and  
26 a method for the protected distribution of certificate and  
27 keying material between a certification authority and an  
28 entity in the certification authority's domain by  
29 establishing a shared secret and using it to protect the  
30 data transferred between the entity and the certifying  
31 authority.

32 The novel features of construction and operation of  
33 the invention will be more clearly apparent during the  
34 course of the following description, reference being had to  
35 the accompanying drawings wherein has been illustrated a  
36 preferred form of the device of the invention and wherein

1     like characters of reference designate like parts  
2     throughout the drawings.

### 3     BRIEF DESCRIPTION OF THE FIGURES

4             FIGURE 1 is a block diagram flowchart showing the  
5     general overall logic flow through a system incorporating  
6     the present invention.

### 7     DESCRIPTION OF THE PREFERRED EMBODIMENT

8             A preferred form of the invention as embodied in a  
9     method and computing system for providing for the protected  
10    distribution of certificate and keying material between a  
11    certification authority and an entity in the certification  
12    authority's domain by establishing a shared secret and  
13    using it to protect the data transferred between the entity  
14    and the certifying authority.

15            In general, as shown in FIGURE 1, the invention is  
16    found in a computer system operating over a network in  
17    accord with the following steps outlined below in detail to  
18    provide for the protected distribution of certificate and  
19    keying material between a certification authority and at  
20    least one entity in the certification authority's domain.

21            The certifying authority begins by generating and  
22    sending keying material, including a password, to the  
23    subject entity via a first secure communications medium.  
24    In this instance, the most secure communications medium is  
25    a non-electronic medium, such as a manual courier, secure  
26    mail or other secure communications medium that is distinct  
27    from the computer system over which the keying material is  
28    to be used as described later in authenticating the entity  
29    to the certifying authority.

30            Once the entity receives the keying material from the  
31    certifying authority, it then generates a public and a  
32    private key pair and protects the public key using the  
33    keying material provided it by the certifying authority.

34            The entity now generates and protects a request for a  
35    certificate to the certifying authority by using the keying

1 material provided it by the certifying authority. Once  
2 generated and protected, the request is sent to the  
3 certifying authority via a second secure communications  
4 medium connecting the certifying authority with the  
5 entities in its certifying domain.

6 Once the certifying authority receives the request  
7 from the entity, the certifying authority authenticates the  
8 identity of the requesting entity. This is done by  
9 requesting, via the second secure communications medium,  
10 that the public key and address of the entity be sent to  
11 the certifying authority.

12 The requesting entity, having received the  
13 authentication request from the certifying authority,  
14 protects the transmission of its selected public key and  
15 address to the certifying authority via the second secure  
16 communications medium, by using the keying material  
17 provided by the certifying authority.

18 Once the identity of the requesting entity is  
19 confirmed, the certifying authority then assembles and  
20 issues the requested certificate to the entity via the  
21 second secure communications medium, and records the public  
22 key of the entity at the certifying authority for public  
23 use by other entities within the certifying domain of the  
24 certifying authority.

25 The invention described above is, of course,  
26 susceptible to many variations, modifications and changes,  
27 all of which are within the skill of the art. It should be  
28 understood that all such variations, modifications and  
29 changes are within the spirit and scope of the invention  
30 and of the appended claims. Similarly, it will be  
31 understood that Applicant intends to cover and claim all  
32 changes, modifications and variations of the example of the  
33 preferred embodiment of the invention herein disclosed for  
34 the purpose of illustration which do not constitute  
35 departures from the spirit and scope of the present  
36 invention.

## WHAT IS CLAIMED IS:

1           1. A method for the protected distribution of  
2           certificate and keying material between a certification  
3           authority and at least one entity in the certification  
4           authority's domain via a communications medium connecting  
5           the certification authority and entities in its domain,  
6           comprising the steps of:

7                 sending keying material, including a password,  
8                 generated by the certifying authority to the entity via a  
9                 first secure communications medium;

10                generating and protecting, by the entity, a public and  
11                a private key pair using the keying material provided the  
12                entity by the certifying authority;

13                generating, protecting and sending via a second secure  
14                communications medium a request for a certificate to the  
15                certifying authority using the keying material provided the  
16                entity by the certifying authority;

17                requesting, by the certifying authority via the second  
18                secure communications medium, that the public key and  
19                address of the entity be sent to the certifying authority;

20                protecting and sending the public key and address of  
21                the entity to the certifying authority via the second  
22                secure communications medium using the keying material  
23                provided it by the certifying authority;

24                assembling and issuing the certificate to the entity  
25                from the certifying authority via the second secure  
26                communications medium and recording the public key of the  
27                entity at the certifying authority for public use within  
28                the domain of the certifying authority.

1           2. The method of claim 1 wherein said step of sending  
2           keying material, including a password, generated by the  
3           certifying authority to the entity via a first secure  
4           communications medium further includes the step of:  
5           selecting the first secure communications medium that is  
6           separate and independent from the second secure  
7           communications medium.

1           3. The method of claim 1 wherein said step of sending  
2     keying material, including a password, generated by the  
3     certifying authority to the entity via a first secure  
4     communications medium further includes the step of:  
5     selecting a non-electronic transmission medium for the  
6     first secure communications medium.



1 / 1

